



BCM RIs 6.0

User Management

Task Based Guide

**Copyright © 2010 Avaya Inc.
All Rights Reserved.**

Notices

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: <http://www.avaya.com/support>

Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](http://support.avaya.com/licenseinfo/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright

Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://support.avaya.com/Copyright>.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support. Web site: <http://www.avaya.com/support>

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://www.avaya.com/support>

Copyright © 2010 ITEL, All Rights Reserved

The copyright in the material belongs to ITEL and no part of the material may be reproduced in any form without the prior written permission of a duly authorised representative of ITEL.

Table of Contents

User Management	5
Overview	5
Required Information	5
Flowchart	6
Accessing Business Element Manager	7
Security Policies	9
Configuring the General Security Policy Settings	10
Configuring Credential Complexity	11
Configuring Lockout on Failed Login	12
Password Expiry	13
Password History	14
Configuring Web Server Certificate, SSH Key Pair, and Challenge Key	15
Managing User Groups	15
Managing User Accounts	19
Adding, Deleting, or Modifying User Accounts	19
Modifying Access to Accounts	23
Avaya Documentation Links	28

User Management

Overview

You can build levels of secure access into your system with the Accounts & Privileges feature, by defining user groups and accounts for all personnel you expect to be doing any type of programming or monitoring of the system. As a security enhancement, you can also set the amount of time that Business Element Manager stays open if there is no input activity. When the period completes, the program automatically returns to the Connect window.

User Groups define a set of actions/functions that can be performed (e.g. VoiceMail administrator). User Accounts are then set up which can have a number of User Groups assigned.

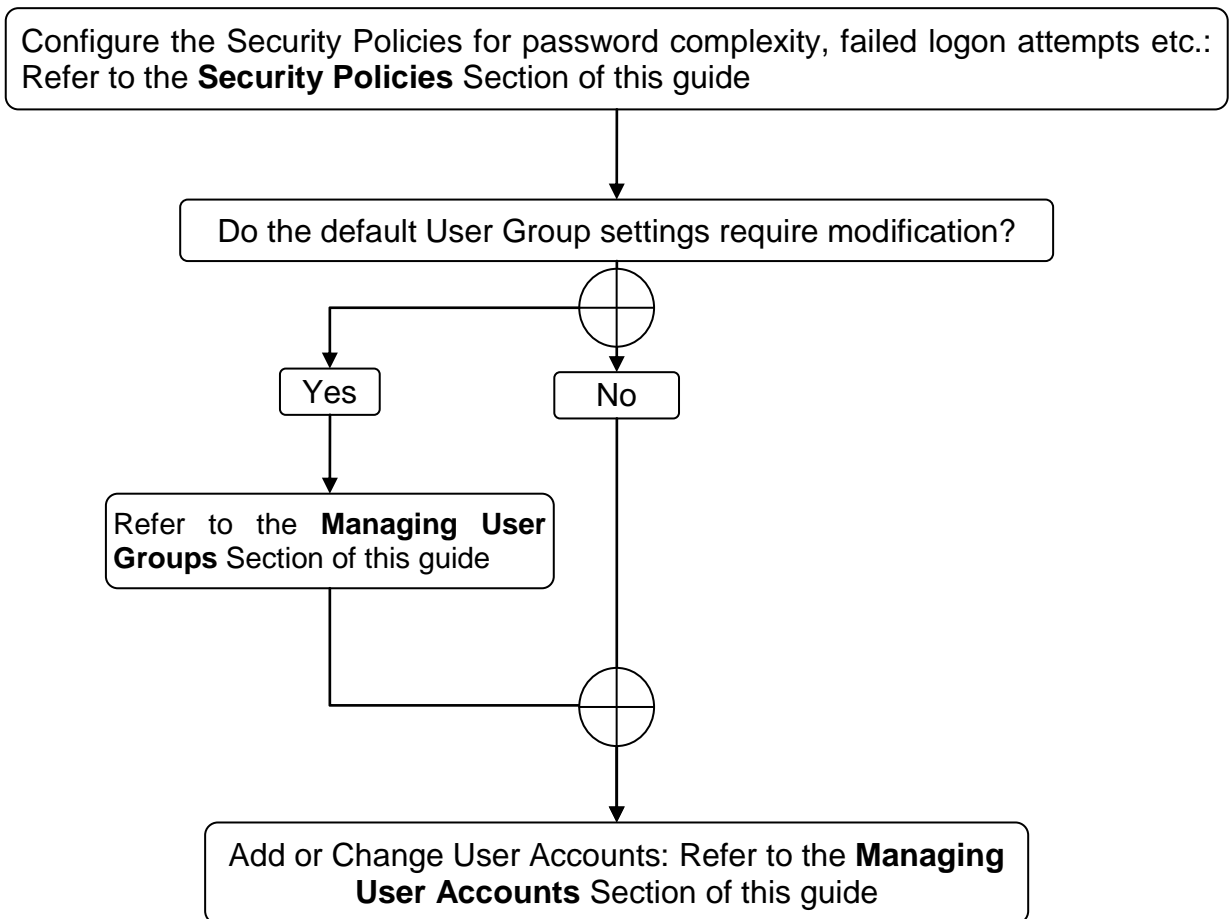
As BCM allows programming via a telephone handset, there is also the option of creating or allowing an existing User Account access to this programming method. Logging on via the telset requires a separate log on ID and password.

Required Information

- Determine what User Groups and User Accounts are required.
- For User Groups, determine what programming access they require.
- Determine whether a Business Element Manager Timeout period is required.
- Determine what password complexity levels are required.

Flowchart

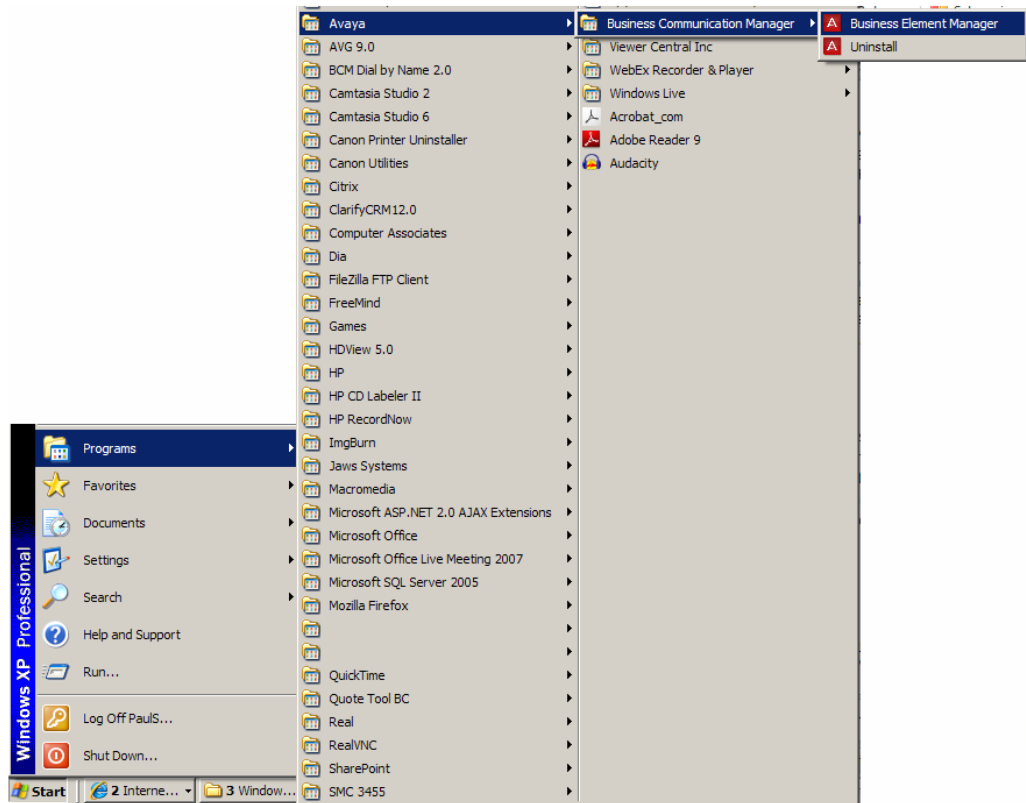
The following flow chart shows the recommended order for configuring User Groups and Accounts.



Accessing Business Element Manager

This section describes how to access the Business Element Manager interface.

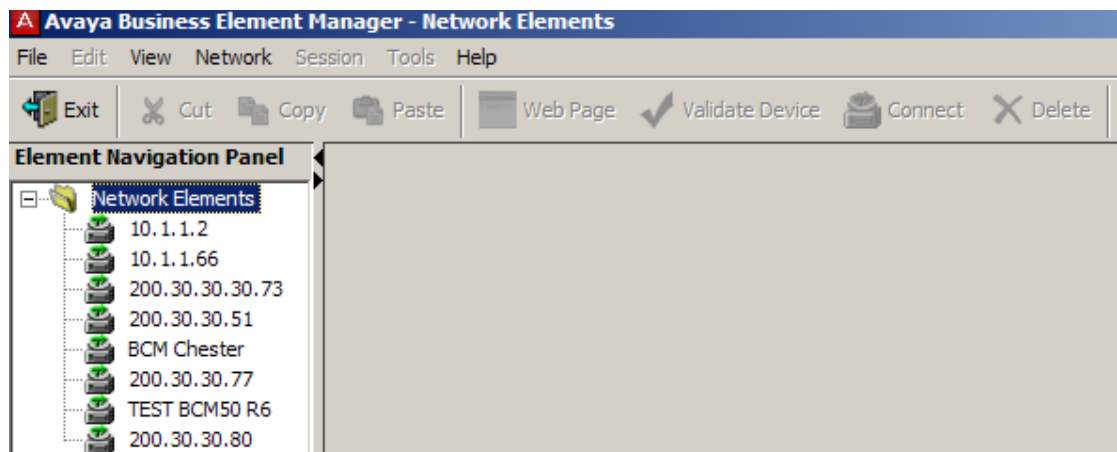
1. To access the Business Element Manager application from the Start Menu, navigate to **Start, Programs, Avaya, Business Communications Manager, Business Element Manager**.



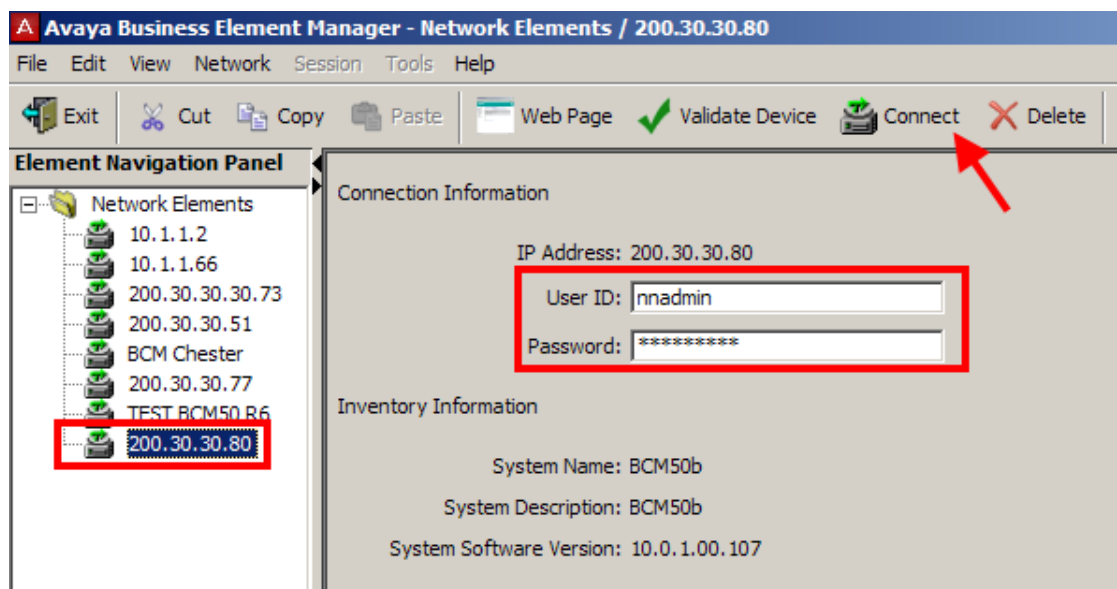
2. Alternatively, double-click on the **Business Element Manager** desktop icon.



3. You will be presented with the **Element Manager** interface.

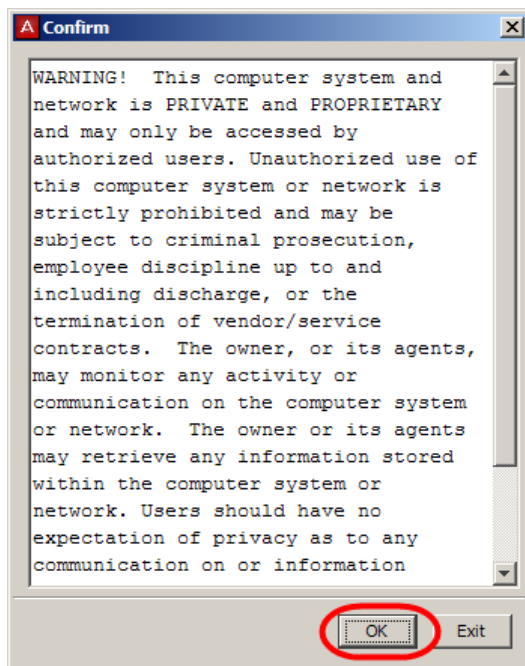


4. Open the **Network Elements** folder and select the IP Address of the BCM.

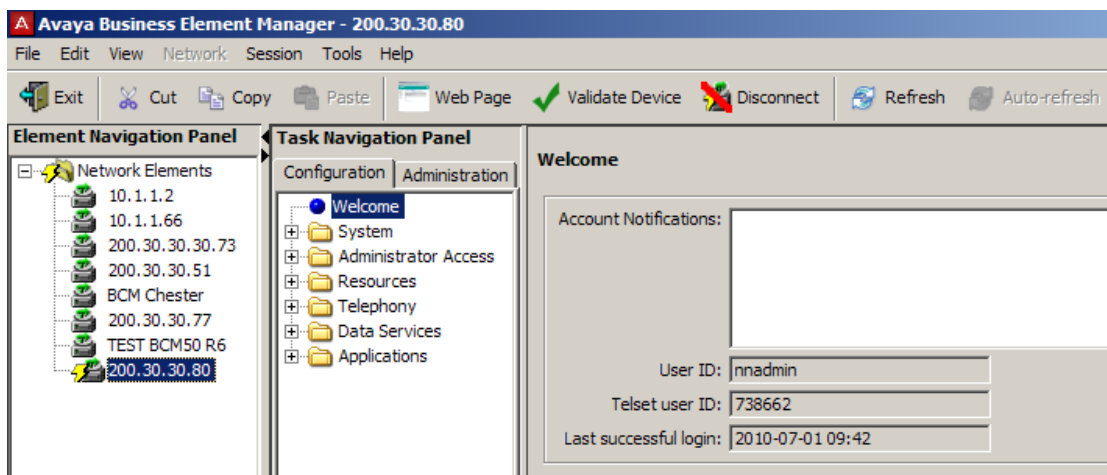


5. Enter the User Name of the BCM in the User Name field, by default this is **nnadmin**. Then enter the Password in the Password field, by default the password is **PlsChgMe!**. Click the **Connect** button.

6. A warning screen will appear, read the warning and click **OK**.



7. You will be presented with the Element Manager interface.



Security Policies

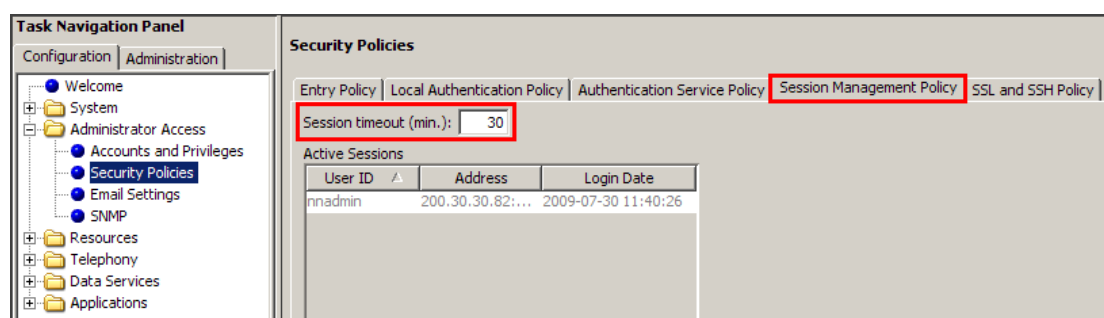
Note: To configure/create any Security Policy or User Groups/Accounts, you must log on to Business Element Manager with an **Account** that has the **Privileges** to do so.

1. Log on to Business Element Manager (refer to the **Accessing Business Element Manager** section of this guide).
2. From the **Configuration** tab, open **Administration Access** and select **Security Policies**.

3. Configure the Security Policy options as required.

Configuring the General Security Policy Settings

There are a number of general security features that can be configured under the Entry Policy. These include a check box to Disable Telset Login feature, and the Disable Post-Login Message check box option. This message can be changed to display the organisations own post-login message. To set Session Timeout go to the Session Management Policy tab.



General Security Policy Settings

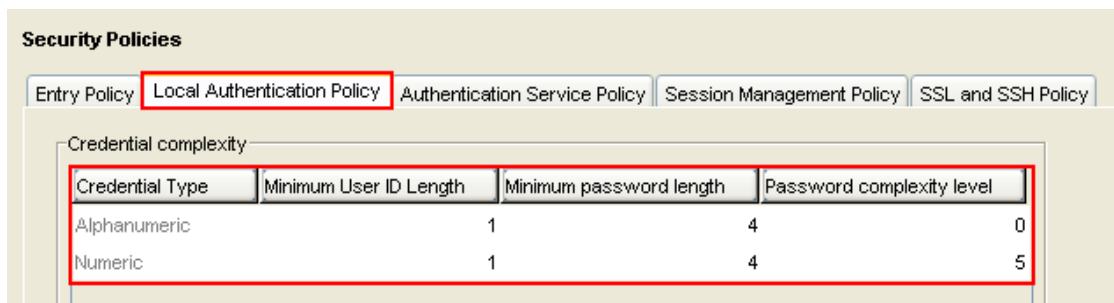
Attribute	Value	Description
Entry Policy Tab		
Disable telset login	check box	When selected, specifies when users cannot access the system through any telset interface. Default: unchecked Tip: If this is enabled, and DHCP changes the system IP address, you can determine the new IP address by way of the OAM port.
Disable post-login Message	check box	When checked, specifies that the post-login security warning will not open on login. Default: not checked
Post login message	text	Displays the post-login security warning. The warning can be edited to customize the message for your system.
Hide Challenge Key	Check box	When selected, display asterisks rather than the characters in the Challenge key
Challenge Key	text	Enter a new Challenge key or use the default Challenge key provided. If you enter a new Challenge key, keep a record of it.

Attribute	Value	Description
Session Management Policy Tab		
Session time out (min.)	minutes	Specifies the number of minutes a logged-in user account can be inactive before the system ends the session and logs out the account. If this field is left blank, the session is only ended when the user logs off.

Configuring Credential Complexity

These settings define the complexity of passwords. There are separate complexity levels for Business Element Manager/CallPilot Manager and telset programming.

1. To configure **Alphanumeric** passwords (i.e. passwords used to login in to Business Element Manager and/or CallPilot Manager Etc.), click on the Local Authentication Policy tab first then the required field of the **Alphanumeric** row.



2. To configure **Numeric** passwords (i.e. passwords used to log on to telset based programming); double-click in the required field of the **Numeric** row.

Credential Complexity Settings

Attribute	Value	Description
Credential Type	Business Element Manager/CallPilot Manager: Alphanumeric Telset: Numeric	Specifies the variety of characters an alphanumeric password must have. The required number of each type is defined by the complexity level. Note: User IDs are not case-sensitive. Telset interface passwords must be numerical. Password complexity for these passwords defines how many unique digits are required.
Minimum User ID length	Alphanumeric 1-32 Telset: Numeric 1-16	Specifies the minimum number of characters that the system requires for each type of credential.
Minimum password length	Alphanumeric 1-32 Telset: Numeric 1-16	Specifies the minimum number of characters that must be entered for a new password. Note: Alphanumeric passwords are case-sensitive. Note: This setting must be the same as or greater than the complexity level setting. Example: If you have a complexity level of two, two different types of characters or two unique numbers, the password must be at least two characters long.

Attribute	Value	Description
Password Complexity Level (Alphanumeric)	1 2 3 4	Defines the number of character types required for an alphanumeric password. Default: 3 1: only one character type is required 2: at least two character types are required 3: at least three character types are required. 4: all four character types are required Note: Check minimum length setting to ensure that it is equal to or greater than the complexity level. Password complexity consists of the following types: <ul style="list-style-type: none"> • upper case alphabet (English) • lower case alphabet (English) • westernized Arabic numbers • non-alphanumeric characters (\$, !, %, ^, period, comma)
Password Complexity Level (Numeric, Telset)	1 2 3 4 5	Specifies the number of unique digits that must be part of a telset password: 1: one unique digit 2: two unique digits 3: three unique digits 4: four unique digits 5: prevent consecutive numbering Note: Check the minimum length setting to ensure that it is equal to or greater than the complexity level.

Configuring Lockout on Failed Login

You can configure lockout periods for users who incorrectly enter log on details a number of times.

Lockout on Failed Login

Enable lockout ☒ Lockout duration (min.)

Lockout counter Lockout counter reset (min.)

Lockout on Failed Login Settings

Attribute	Value	Description
Enable lockout	check box	When checked, specifies that enable lockout rules apply.
Lockout counter	digits	Specifies the number of times the user can attempt to enter an invalid password before the user is locked out. Default: 25; for increased security, set this number to 5.
Lockout duration (min)	minutes	Specifies the amount of time after the user is locked out before they are allowed to login again. Reset the lockout counter to zero. Default: 30
Lockout counter Reset (min)	minutes	Specifies the number of minutes after a lockout before the lockout counter is automatically reset to zero. Default: 30 Example: If the lockout counter reset is set at 30 minutes and a user enters invalid passwords, but does not reach the lockout counter threshold, then waits 30 minutes before trying again, the lockout counter resets and begins

Attribute	Value	Description
		counting from 1 again. If the user enters invalid passwords until the lockout counter threshold is reached, the Lockout duration determines when the user can sign back onto the system.

Password Expiry

The Password Expiry parameters can be configured with expiry policies for accessing the BCM.

Security Policies

Entry Policy | **Local Authentication Policy** | Authentication Service Policy | Session Management Policy | SSL and SSH Policy

Credential complexity

Credential Type	Minimum User ID Length	Minimum password length	Password complexity level
Alphanumeric	1	8	3
Numeric	1	4	5

Lockout on Failed Login

Enable lockout: ☒ Lockout duration (min.): 30

Lockout counter: 25 Lockout counter reset (min.): 30

Password Expiry

Enable Password Expiry: ☐

Days before password expire: 90

Warning days before password expire: 10

Password History

Enable password history: ☐

Password history length: 5

Attribute	Description
Enable check box	To enable the password expiry policy
Days before password expire	Enter the number of days that you can use a password before it expires.
Warning days before password expire	Enter the number of days prior to password expiry that the user receives a notification

Password History

The password history feature can be used to prevent users from re-using the same password. Administrators can configure the number of previous passwords to store and check.

Security Policies

Entry Policy Local Authentication Policy Authentication Service Policy Session Management Policy SSL and SSH Policy

Credential complexity

Credential Type	Minimum User ID Length	Minimum password length	Password complexity level
Alphanumeric	1	8	3
Numeric	1	4	5

Lockout on Failed Login

Enable lockout: ☒ Lockout duration (min.): 30

Lockout counter: 25 Lockout counter reset (min.): 30

Password Expiry

Enable Password Expiry: ☐

Days before password expire: 90

Warning days before password expire: 10

Password History

Enable password history: ☐

Password history length: 5

Attribute	Description
Enable Password History check box	To enable the password history
Password history length	Enter the number of previous passwords to store and check for an account...

Configuring Web Server Certificate, SSH Key Pair, and Challenge Key

SSL This procedure allows you to upload a private security certificate to replace the generic web certificate provided with BCM. Using a custom site-specific certificate, you can have site validation which will eliminate the security warnings.

Transferring an SSH Key-Pair allows the administrator to download a public security certificate or an SSH key-pair. The new certificate must be installed on each SFTP server the BCM communicates with to ensure a secure connection for operations like backup and restore, and software updates.



Web Server Certificate and Challenge Key Settings

Attribute	Description
Install Web Server Certificate (button)	Opens the file system browser to allow a system-specific security certificate and the accompanying Private key to be selected. Downloads application security certificates to the server where SSH is running to ensure a secure copy connection for operations like backup and restore, upgrades and patches.

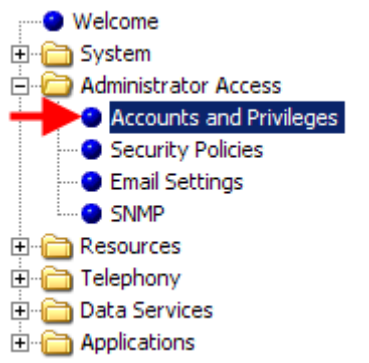
Managing User Groups

User Groups have assigned Group Privileges which define what functions a user can perform. There are many pre-defined groups available, which have varying assigned Privileges. For example, the Administrator Group has all 35 listed Privileges assigned, whereas the Power Users group has 5 of the 35 Privileges assigned.

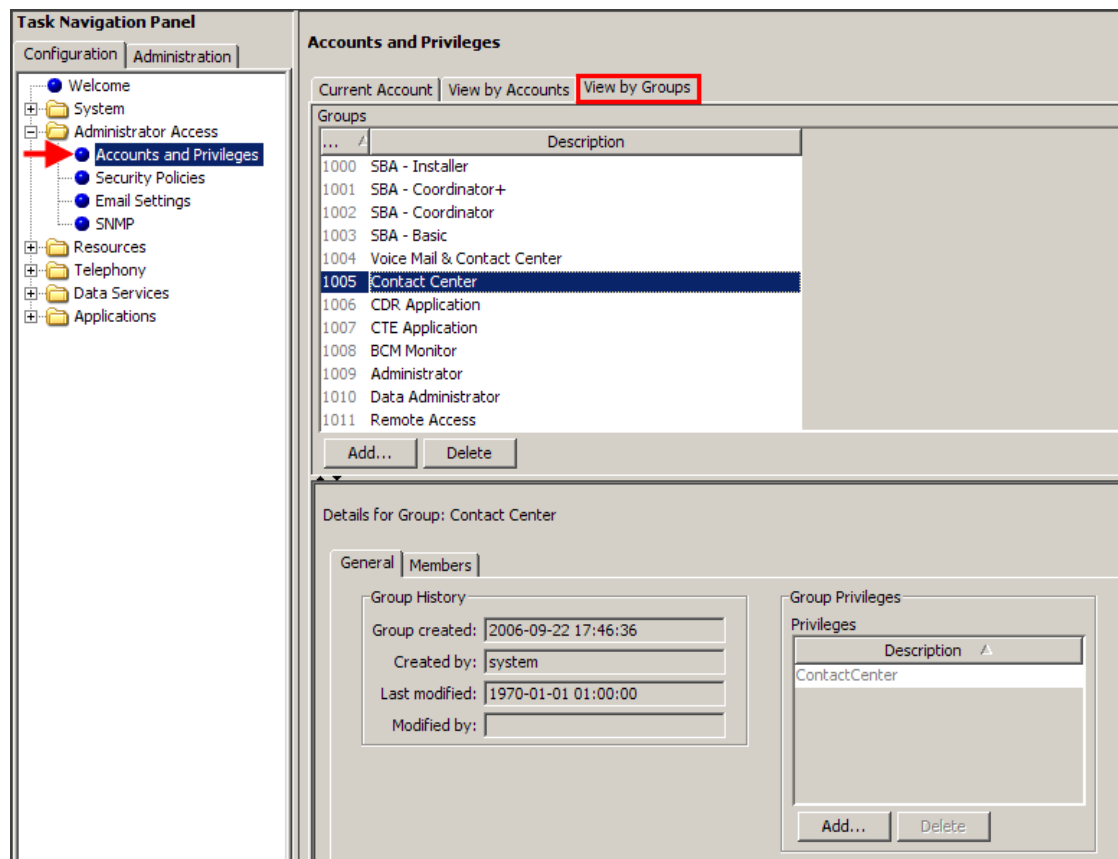
Use the following procedure to Add, Delete, or Change User Groups:

1. Log on to Business Element Manager (refer to the **Accessing Business Element Manager** section of this guide).

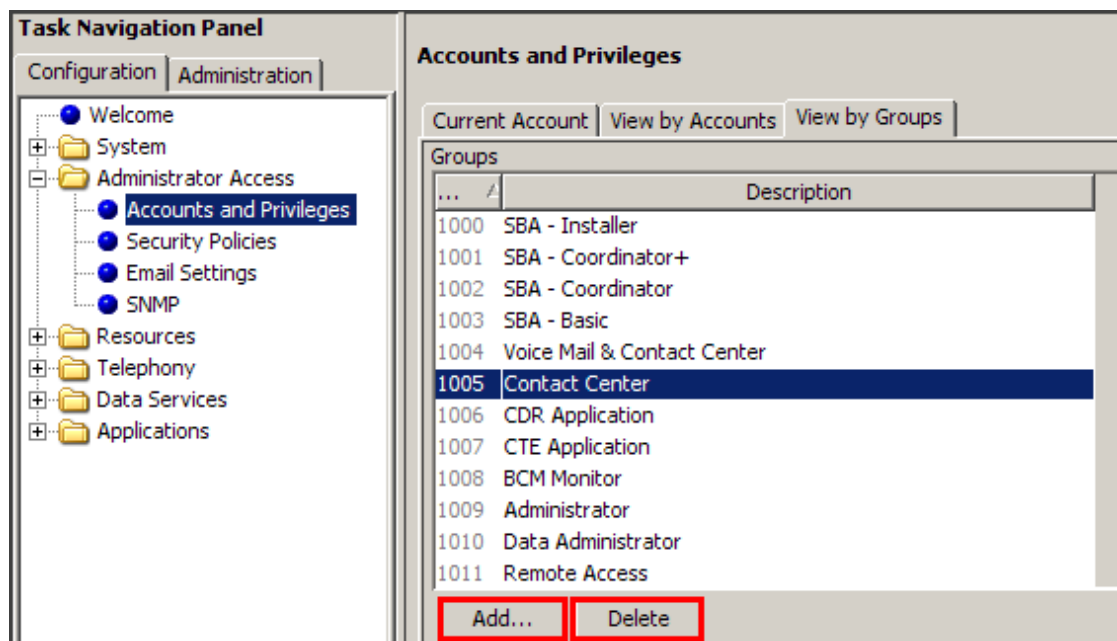
- From the **Configuration** tab, open **Administrator Access** and select **Accounts & Privileges**.



- Click on the **View by Groups** tab.



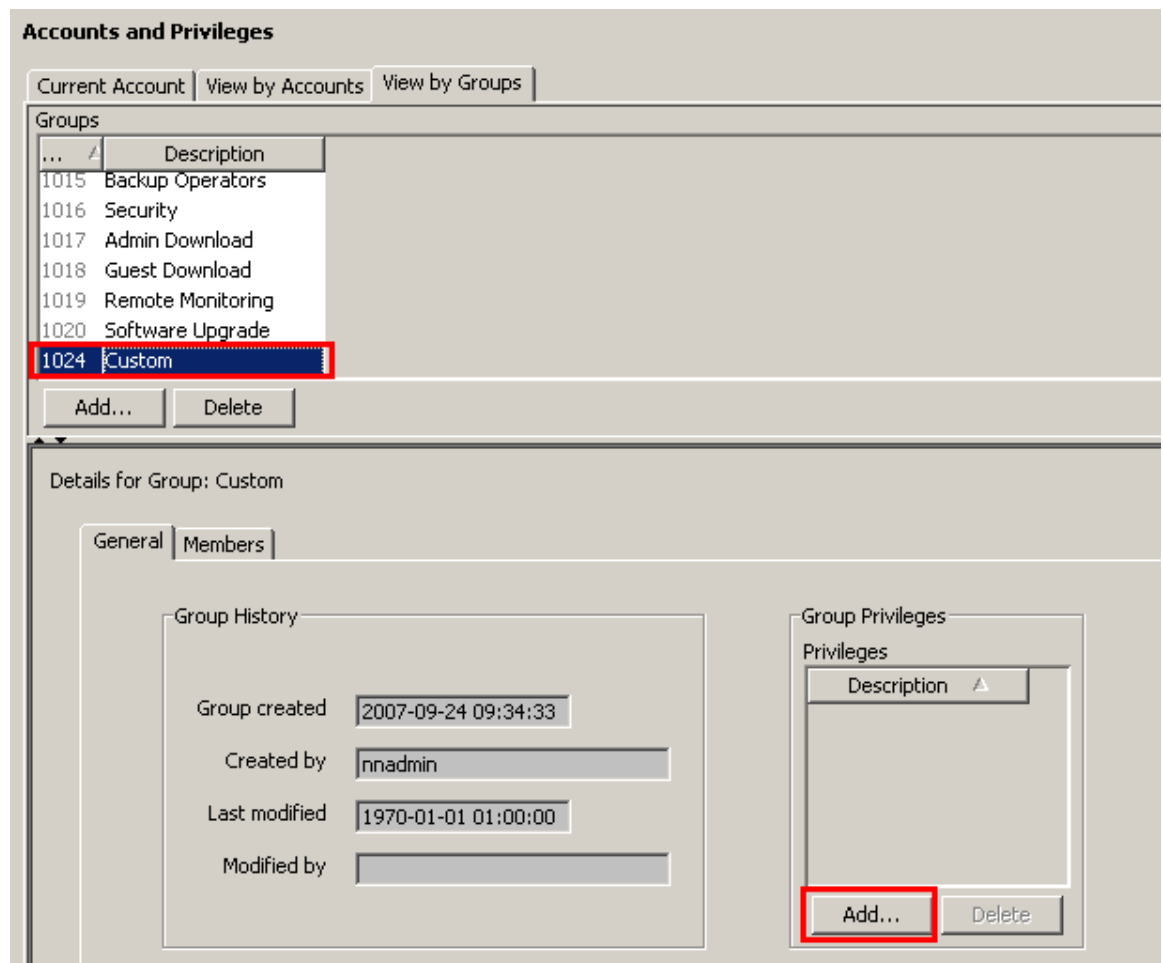
4. To delete a group, select the group and click **Delete**.



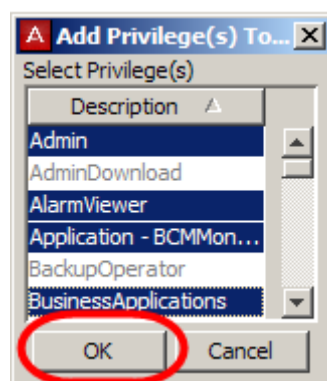
5. To add a new group, click **Add** underneath the **Groups** window. Enter a name for the Group. Click **OK**.



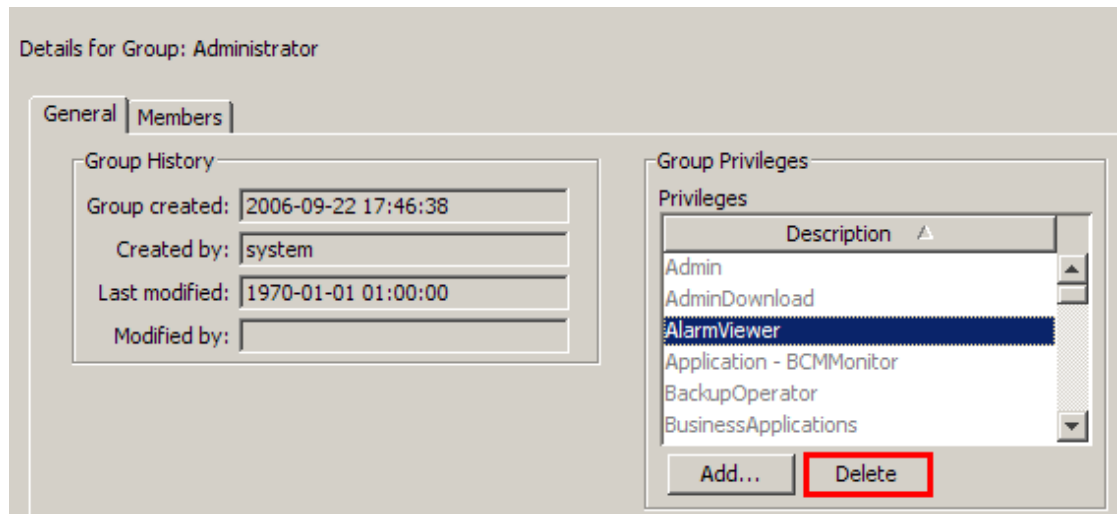
6. The Group will be added to the **Groups** list. In the **Group Privileges** window, select **Add**.



7. Select the Privileges required for this group and click **OK**. (By use of the Ctrl key and the mouse it is possible to select multiple Group Privileges, hold down Ctrl Key and click on selected properties to select.)



8. If you need to delete any Privileges from the **Group Privileges** list, simply select the Privilege and click **Delete**.



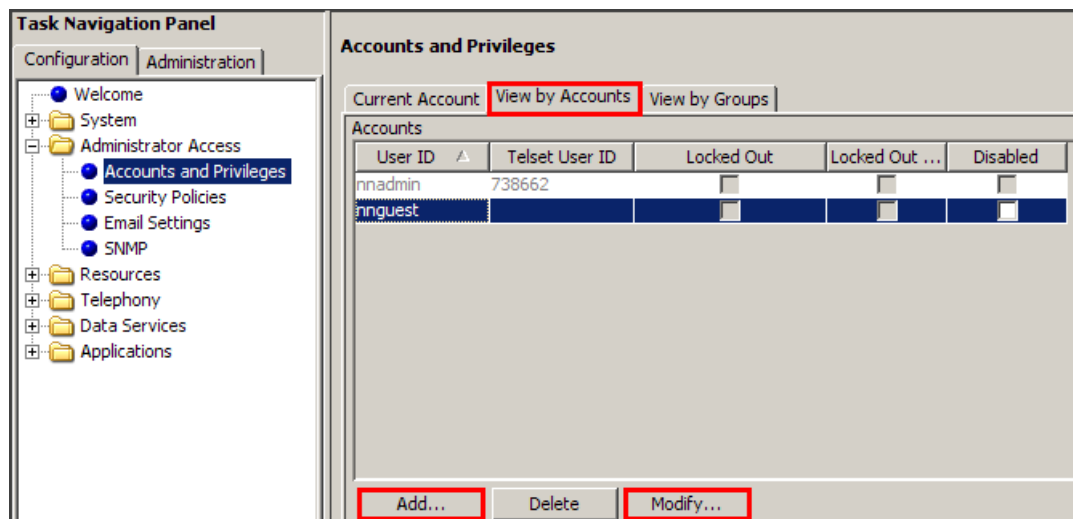
Managing User Accounts

From the View by Accounts screens you can set up or modify User Accounts, set the User ID & passwords for Business Element Manager/CallPilot Manager, and assign User Groups to the User Account.

Adding, Deleting, or Modifying User Accounts

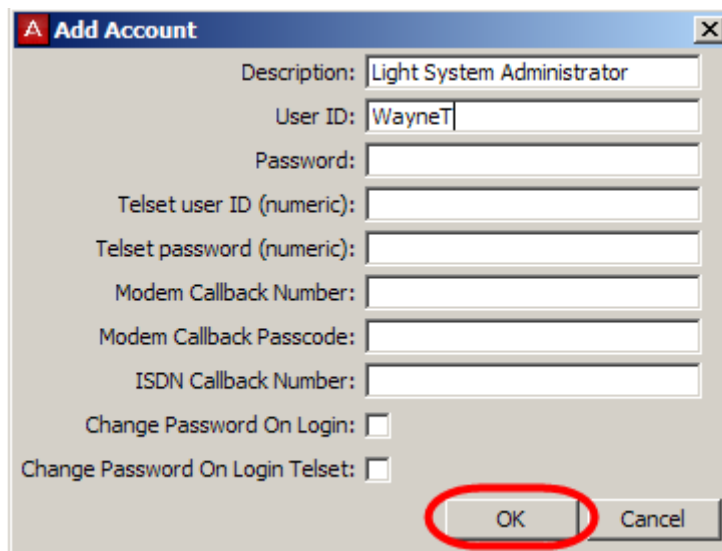
Use the following procedure to Add, Delete, or Modify User Accounts:

1. Log on to Business Element Manager (refer to the **Accessing Business Element Manager** section of this guide).
2. From the **Configuration** tab, open **Administrator Access** and select **Accounts & Privileges**.
3. Click on the **View by Accounts** tab.



4. Click on **Add** to add a new user, or select an existing user and click **Modify**.
5. Enter a brief **description** (optional), and then any or all of the following:
 - a. A **User ID & Password** for Business Element Manager/CallPilot Manager access.
 - b. A numerical **Telset User ID & Telset Password** to allow this user to program via a telephone handset.
 - c. A **Callback Number** (telephone number, optional i.e. you may not wish to use callback) and **Callback Passcode** if this account is to be used for remote support.

Note: Anytime a password is entered, you will be asked to re-enter that password for confirmation.



6. Click **OK** to save the new/changed details. If you have added a new account, the account will appear in the **Accounts** list.

7. To assign a User Group to the selected account, click on the **Group Membership** tab in the lower window.

Accounts and Privileges

Current Account | View by Accounts | View by Groups

Accounts

User ID ▲	Telset User ID	Locked Out	Locked Out ...	Disabled
WayneT		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
nnadmin	738662	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
nnquest		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add... Delete Modify...

Details for Account: Light System Administrator

General | Remote Access | History | **Group Membership**

Description: Light System Administrator

Account Expiry

Account will be disabled on: 1970-01-01 01:00

Enable account expiry: ☐

Account Textual Credentials

Password Expiry:

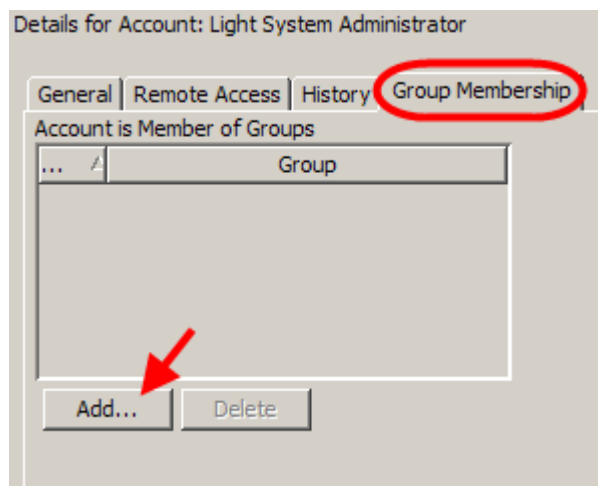
Change Password On Login: ☐

Account Telset Credentials

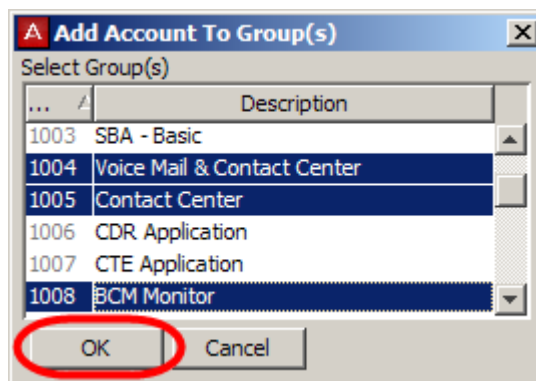
Password Expiry:

Change Password On Login: ☐

8. To add a User Group to this account, click **Add**.



9. Select the groups to be assigned to this account (you may wish to use the shift and/or ctrl keys to select multiple accounts), and click **OK**.



10. These groups will be added to the **Account is Member of Groups** list.

Accounts and Privileges

Current Account | View by Accounts | View by Groups

Accounts

User ID ▲	Telset User ID	Locked Out	Locked Out ...	Disabled
WayneT		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
nnadmin	738662	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
nnquest		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add... Delete Modify...

Details for Account: Light System Administrator

General | Remote Access | History | Group Membership

Account is Member of Groups

...	Group
1004	Voice Mail & Contact Center
1005	Contact Center
1008	BCM Monitor

Add... Delete

Modifying Access to Accounts

There are a range of options for modifying access for an account. An account can be disabled, have an expiry date and time limit set against it for access. Also Locked-out Accounts due to incorrect password entry can be unlocked.

Also, if you are logged in as an Administrator (i.e. your account has the Administrator group assigned to it), you can set exclusive access whilst you are logged in for maintenance or special activities. This prevents anybody else from logging in but does not affect users currently logged-in.

To Disable a User Account

1. Log on to Business Element Manager (refer to the **Accessing Business Element Manager** section of this guide).
2. From the **Configuration** tab, open **Administrator Access** and select **Accounts & Privileges**.
3. Click on the **View by Accounts** tab.

- For the account you wish to disable, click in the **Disabled** checkbox.

Accounts and Privileges

Current Account View by Accounts View by Groups

Accounts

User ID	Telset User ID	Locked Out	Locked Out Telset	Disabled
RemAss		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wayne		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
admin		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
administrator		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
nnadmin	738662	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
nnguest		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
user31		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
user32		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- To re-enable the account, clear the check box.

Unlocking a Locked-out Account

An Account will be locked if a user has incorrectly entered their password, beyond the lockout counter threshold.

Use the following procedure to unlock a locked Account:

- Log on to Business Element Manager (refer to the **Accessing Business Element Manager** section of this guide).
- From the **Configuration** tab, open **Administrator Access** and select **Accounts & Privileges**.
- Click on the **View by Accounts** tab.
- For the account you wish to unlock, clear the **Locked Out** check box.

Accounts and Privileges

Current Account View by Accounts View by Groups

Accounts

User ID	Telset User ID	Locked Out	Locked Out Telset	Disabled
RemAss		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wayne		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
admin		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
administrator		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
nnadmin	738662	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
nnguest		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
user31		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
user32		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Setting an Access Time Limit for an Account

If you wish to only allow temporary access for an account, use the following procedure:

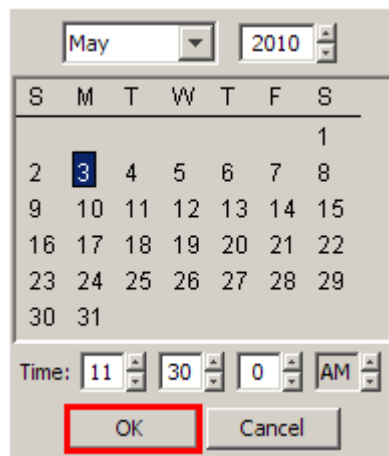
1. Log on to Business Element Manager (refer to the **Accessing Business Element Manager** section of this guide).
2. From the **Configuration** tab, open **Administrator Access** and select **Accounts & Privileges**.
3. Click on the **View by Accounts** tab.
4. Select the **Account** you wish to apply the time limit to.
5. In the lower window, select the **General** tab.
6. Click the **Enable Account Expiry** check box.

The screenshot shows the 'Accounts and Privileges' window. At the top, there are tabs for 'Current Account', 'View by Accounts', and 'View by Groups'. Below these is a table of accounts:

User ID	Telset User ID	Locked Out	Locked Out ...	Disabled
nnadmin	738662	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
nnquest		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Below the table are buttons for 'Add...', 'Delete', and 'Modify...'. The 'Details for Account:' section is expanded, showing the 'General' tab. It includes a 'Description' text area, an 'Account Expiry' section with a date-time picker set to '2009-01-01 01:00:00' and an 'Enable account expiry' checkbox, and an 'Account Textual Credentials' section with a 'Password Expiry' date-time picker set to '2009-01-01 01:00:00' and a 'Change Password On Login' checkbox.

- Click in the **Account will be disabled on** field, and set the expiry date and time in the date/time selection screen.



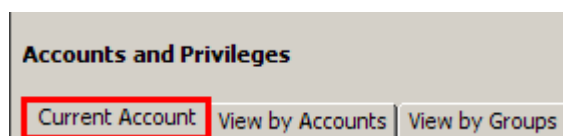
A date and time selection dialog box. At the top, there are dropdowns for the month (May) and year (2010). Below is a calendar grid for May 2010. The day 3 is selected and highlighted in blue. At the bottom, there are spinners for the time: 11:30 AM. The OK button is highlighted with a red rectangular box.

- Click **OK** to save the selection.

Enabling Exclusive Access Whilst Logged in as an Administrator

If you are logged in with an Account that has Administrator privileges, you can enable exclusive access. This may be necessary to prevent other users logging in whilst you are performing essential maintenance.

- Log on to Business Element Manager (refer to the **Accessing Business Element Manager** section of this guide).
- From the **Configuration** tab, open **Administrator Access** and select **Accounts & Privileges**.
- Select the **Current Account** tab.



A dialog box titled "Accounts and Privileges". It contains three tabs: "Current Account", "View by Accounts", and "View by Groups". The "Current Account" tab is selected and highlighted with a red rectangular box.

- Click on the **Enable Exclusive Access** button.

Accounts and Privileges

Current Account | View by Accounts | View by Groups

This panel is refreshed at login.

Account Notifications:

User ID: nnadmin

Password: *****

Telset user ID: 738662

Telset password: *****

Last successful login: 2010-07-02 10:42

Account Management: Local Authentication

Failed Login History

Last failed login: 2010-06-24 15:44

From:

Failed Telset Login History

Last failed login:

From:

Exclusive access

Enable Exclusive Access... | Disable Exclusive Access

Exclusive access time remaining (sec.): 0

- Set the duration you require for Exclusive Access and click **OK**.
- Exclusive Access will expire after this time, or when you have finished the maintenance function click the **Disable Exclusive Access** button.

Exclusive access

Enable Exclusive Access... | **Disable Exclusive Access**

Exclusive access time remaining (sec.): 0

Avaya Documentation Links

- Administration and Security